FILE NO.: A34941 - 066340.0141

BAKER BOTTS L.L.P
30 ROCKEFELLER PLAZA
NEW YORK, NEW YORK 10112

TO ALL WHOM IT MAY CONCERN:

Be it known that I, Wolfram Drescher, a citizen of Germany, whose post office address is Alaunplatz 2, D-01099 Dresden, Germany has made an invention in

PROCESS AND APPARATUS FOR FINITE
FIELD MULTIPLICATION (FFM)

of which the following is a

SPECIFICATION

BACKGROUND OF THE INVENTION

[0001] The invention relates to a process for performing a finite field multiplication of a first Galois element a represented by a bit vector $a_0...a_{n-1}$ in a first input register, to be multiplied by a second Galois element b represented by a bit vector $b_0...b_{n-1}$ in a second input register in a digital Galois multiplier (MUL), the Galois elements a and b being members of a Galois field GF 2^n described by an irreducible polynomial PR having a bit representation $PR_0...PR_n$.

[0002] In finite field multiplication of Galois elements, it is premised that the basic arithmetical operation in digital signal processing is specified in general by:

$$y = \sum_{i=0}^{n} x_i * a_i$$

Many algorithms can be reduced in essence to this folded sum, or arithmetically speaking, the summation across products. Usually in digital signal processing, these algorithms, e.g. in digital signal processors (DSP), are accelerated by the realization of a hard-wired hardware circuits implementing this summation of products. Such subassemblies are commonly referred to as multipliers (MUL).

[0003] If in this multiplier the arithmetic is applied in residue class fields with their modulo operation, use is made of a Galois MUL performing a finite field multiplication, in that in each line of the multiplier, first a partial product $a \times b_i$ ($i = 0$ to $n-1$) is formed. Then the partial product is added to the sum of the preceding lines, before the modulo operation is performed. This is done by adding bit places $PR_0 \ldots PR_{n-1}$ to the sums previously computed, in accordance with an overflow occurring in the preceding line.

[0004] The invention relates further to one circuit apparatus each for carrying out the above-mentioned process according to Claims 1 to 3, and to one circuit apparatus in which a Galois multiplier accumulator (MAC) is arranged, in which each of the said circuit apparatuses is contained.

[0005] A Galois MUL of cellular structure was described in "A Cellular Array Multiplier for GF(2^m)," *IEEE Transactions on Computers*, Dec. 1971, 1573-1578, by B.A. Laws and C.K. Rushforth. In "Efficient Semisystolic Architectures for Finite Field Arithmetic," *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems*, vol. 6 no. 1, March 1988, pp. 101-113, Surendra K. Jain, Leilei Song and Keshab K. Parhi tabulate various algorithms for the realization of Galois multipliers and their representation in circuitry.

[0006] A disadvantage of the realizations previously specified is that they possess a high 'logical depth,' i.e. a multitude of gates to be traversed in succession, and therefore, long signal transit times occur upon their implementation in finite field multiplication.

[0007] The object of the invention is to accelerate finite field multiplication.

SUMMARY OF THE INVENTION

[0008] The process side solution to this problem provides that in a first part of the Galois MUL, an addition part, in one process step an intermediate result Z of intermediate sums of partial products of bit width 2n - 2 is formed, which does not represent any element of the Galois field described by an irreducible polynomial PR, and that in a second part of the Galois MUL, a reduction part, the intermediate result Z having bit places $Z_{2n-2} \ldots Z_0$ is processed by means of a modulo division by the irreducible polynomial PR having bit places $PR_{n-1} \ldots PR_0$, and after traversing all XOR connections, the result E with bit places $E_{n-1} \ldots E_0$ is computed.

[0009] In this solution according to the invention, a tree structure is realized in the addition part, operating more rapidly than in the prior art by virtue of its parallel signal processing.

[0010] An advantageous modification of the process side solution provides that in a reduction part, the modulo division of the intermediate result Z by the irreducible polynomial PR is carried out in two steps, all bit places $Z_{2n-2} \ldots Z_n$ are respectively AND connected in a first process step with an expanded form PE of the irreducible polynomial PR, with bit places

$PE_{n-1}...PE_0$, and then, by means of a first parallel-operating adder tree structure effectively realizing the operation XOR, and then assembled.

[0011] These assembled partial results are subsequently AND connected in a second processing step with bit places $PR_{n-1}...PR_0$ of the irreducible polynomial PR, and they are respectively connected by a second parallel-operating adder tree structure that also realizes the logical operation XOR effectively performed, in each instance to the bit places $Z_{n-1}...Z_0$ of the intermediate result Z to yield the result E with bit places $E_{n-1}...E_{0.}$

[0012] This solution according to the invention reflects the realization that in the reduction part also, by a two-stage paralleling of the signal paths, the signal transit times are additionally reduced.

[0013] A highly advantageous solution to the problem according to the invention provides that a matrix PEM of bit place arrangement

$$PEM =: \begin{pmatrix} PE_{n-1,n-2} & \cdots & PE_{n-1,0} \\ & \cdots & \\ PE_{0,n-2} & \cdots & PE_{0,0} \end{pmatrix}$$

is precalculated with respect to the expanded form PE of the irreducible polynomial PR in the Galois field GF 2^n, that in the reduction part the modulo division of the intermediate result Z by the irreducible polynomial PR is performed in that all bits $Z_{2n-2}...Z_n$ are each AND connected to the matrix PEM of the expanded form PE of the irreducible polynomial PR with bit places $PE_{n-1,n-2}...PE_{n-1,0}...PE_{0,n-2}...PE_{0,0}$, and then, by means of a third parallel-operating adder tree structure realizing the logic operation XOR, assembled to form the result E.

[0014] In this solution according to the invention, an additional transit time curtailment is effected, in which all bit places $Z_{2n-2}...Z_n$ of the intermediate result Z are AND connected by a precalculated data set of expanded form PEM of the irreducible polynomial, which are processed matrixwise in the reduction part of the Galois MUL, and then assembled in a single-step third parallel adder tree structure.

[0015] This application of the precalculated expanded irreducible polynomial in the modulo operation is effected by the single-step processing in the reduction part with special acceleration for the performance of the finite field multiplication.

[0016] An advantageous embodiment of the solution to the problem according to the invention provides that for variable Galois elements va<a and vb<b, with a resulting bit width 2m - 2 of the intermediate result Z for adaptation to different Galois fields, all bit places of the intermediate result Z, before being connected to the expanded form PE of the irreducible polynomial PR, are shifted by $Z_{2mmax-2} - Z_m$ places by means of a decoder and field size adaptation logic, the bit width 2mmax representing the maximum bit width of the intermediate result Z for maximal bit width n of each of the Galois elements a and b.

[0017] In this solution, account is taken of the fact that the Galois MUL is made programmable and hence adaptable to the size of its processing tasks. This is accomplished in that leading zeroes not taken into account in the processing operations, by left shift of the operands when put into the Galois MUL.

[0018] An apparatus-wise advantageous embodiment of the solution to the problem according to the invention provides that a Galois multiplier accumulator (MAC) be arranged, that contains the Galois MUL, the first and second input registers, the expanded form PE and/or the irreducible polynomial PR, or the "preset register bank" containing the matrix PEM, the result register, and an adder, the output of the Galois MUL being connected to an input of the adder. Its output in turn is connected to an input of the first input register and/or an input of the second input register.

[0019] In this apparatus-side solution, the advantageous application of the Galois MUL according to the invention within a Galois multiplier accumulator (MAC) is of complex conformation.

[0020] The invention will be illustrated below in more detail in terms of an embodiment by way of example.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 shows a block diagram of a Galois MUL with bit multiplier and partial product adder in the addition part, and a reduction part with modulo reduction apparatus.

Fig. 2 shows a block diagram of a Galois MUL with bit multiplier and partial product adder in the addition part, and in the reduction part, a reduction two-step adder apparatus realizing the Q-reduction adder part and final adder part.

Fig. 3 shows a block diagram of a Galois MUL with bit multiplier and partial product adder in the addition part, and in the reduction part with reduction single-step adder apparatus.

Fig. 4 shows a block diagram of a Galois MUL with bit multiplier and partial product adder in the addition part, and reduction part with decoder and field-size adaptation logic.

Fig. 5 shows a circuit diagram of a partial product adder key configuration.

Fig. 6 shows a circuit diagram of a modulo reducer configuration.

Fig. 7 shows a circuit diagram of a two-step adder key configuration.

Fig. 8 shows a circuit diagram of a single-step adder key configuration.

DETAILED DESCRIPTION OF THE INVENTION

[0021] As may be seen in Fig. 1, in the first input register 1 a stored Galois element a and a Galois element b stored in the second input register 2 are furnished for the Galois MUL 20. The input goes into the addition part 105 of the Galois MUL 20, which also includes a reduction part 106. This reduction part 106 has the form of a modulo reduction apparatus 107. Within the Galois MUL 20, the addition part 105 generates an intermediate result for modulo processing in the modulo reduction apparatus 107. In addition, at the input of the modulo reduction apparatus 107, the stored irreducible polynomial PR 9 is made available.

[0022] The addition part 105 consists of a bit multiplier 3 and a partial product adder 4. The Galois elements a and b put into the Galois MUL 20 are individually multiplied out in the bit multiplier 3 with respect to their place values. They are made available as individual partial products to the partial product adder 4, in which they are additively assembled to yield the individual place values $Z_{2n-2}...Z_0$. The addition part 105 consists in its apparatus of the partial product adder expansion structure 16 and the partial product adder key configuration 19.

[0023] The intermediate result Z is modulo combined with the value of the stored irreducible polynomial PR 9 in the modulo reduction apparatus 107, and can here be made available at the output with the value E for the adjoined result register 10.

[0024] The modulo reduction apparatus 107 consists in its apparatus of a modulo reduction expansion structure 17 and the modulo reducer key configuration 18.

[0025] As may be seen in Fig. 2, the structure and mode of operation of the addition part 105 of the Galois MUL here described are coincident with that described in Fig. 1. In departure therefrom, to perform the modulo connection, here a precalculated expanded form PE 7 of the irreducible polynomial PR 9 is connected to carry out the modulo connection in the reduction part 106.

[0026] This expanded form PE 7 of the irreducible polynomial PR 9 is computed in three partial steps, subject to the convention:

- p(0) designates the MSB and p(n) the LSB of the irreducible polynomial;
- n is a field quantity.

[0027] The terms are computed with the matrix

$$Z^{nxn} = \begin{matrix} (Z_{11} \dots Z_{1n}) \\ : \qquad : \\ (Z_{n1} \dots Z_{nn}) \end{matrix}$$

and applied to the following routine:

1. Initializing the matrix Z_{11}: = 1, setting all other elements of the lst line to zero, Z_{1j}: = 0, where j = 2 ... n

2. Calculation of lines i = 2 ... n using the recursive formula Zi, j = $Z_{(i-1),(j+1)}$ XOR (p(j) AND $Z_{(i-1),1}$) where i = 2 ... n, j = 1 ... n - i + 1

3. Reading off the preset terms $r(i-1) = Z_{i,1}$, where $i = 1 \dots n$, and storing in the preset register 7

The reduction part 106 processing the intermediate result Z is here of two-step form, consisting of Q reduction adder part 5 and final adder part 6.

[0028] In the Q reduction adder part 5, all place values $Z_{2n-2} \dots Z_n$ of the intermediate result Z present at its input are AND connected respectively to the bit places of the expanded polynomial, modulo added line by line in Q reduction adders, and these values made available for further processing in the subsequently adjoined final adder part 6. Here they are each AND connected to the bit places of the irreducible polynomial PR 9 adjoined at the input of the final adder part 6, and then these values are assembled columnwise together with the place values $Z_{n-1} \dots Z_0$ of the intermediate result Z in the final adder part 6 by modulo addition, and given out at the output of the final adder part 6 to the result register 10.

[0029] The reduction two-step adder apparatus 110 consists, in its apparatus, of the two-step adder key configuration 109 and the two-step adder expansion structure 108.

[0030] As may be seen in Fig. 3, the structure and mode of operation of the addition part 105 of the Galois MUL 20 here described coincide with that described in Figs. 1 and 2. In departure therefrom, to perform the modulo connection in the reduction part 106, instead of irreducible polynomial PR 9, or expanded form PE 7, a "preset register bank" 12 is here employed in place of irreducible polynomial PR 9 or expanded form PE 7, in which a matrix PEM 11 of precalculated terms of the irreducible polynomial is stored.

[0031] The calculation of the preset terms to be applied in this reduction single-step adder apparatus 113 is subject to the convention:

- P0 designates the LSB of the irreducible polynomial PR 9
- PR_{ij} designates the j-th preset term for calculating the i-th result
- n designates field size

[0032] The following routine is used:

$$PR_{ij} = (r_{j-1} \text{ AND } P_i \text{ XOR } r_{j-2} \text{ AND } P_{i-1} \text{ XOR } \ldots \text{ XOR } r_{j-i-1} \text{ AND } P_0)$$

When a subscript of the r-terms or P-terms becomes <0, the calculation is broken off.

[0033] The reduction part 106 processing the immediate result Z is realized by the reduction one-step adder apparatus 113. In it, all place values $Z_{2n-2}...Z_n$ of the intermediate result Z present at its input are each AND connected with the matrix of bit places of the adjoined preset register bank 12, and then these values are assembled line by line together with the respective place values $Z_{n-1}...Z_0$ of the intermediate result Z modulo additively in adders, and at the outputs of the adders the result is made available to the result register 10.

[0034] The reduction one-step adder apparatus 113 consists in its arrangement of the one-step adder key configuration 112 and the one-step adder expansion structure 111.

[0035] As may be seen in Fig. 4, the structure and the mode of operation of the Galois MUL 20 here described differ from the ones described in Figs. 1 and 2 in that, in addition, a decoder 14 and a field-size adaptation logic 13 are employed in the processing of the intermediate result Z in the reduction part 106.

[0036] According to the bit width of the Galois elements stored in the first input register 1 and in the second input register 2, after processing in the addition part 105 upon occurrence of leading zeroes in the intermediate result Z, the bit place occupants of Z are left-shifted until no leading zeroes occur in the further processing of the intermediate result. In the field-size adaptation logic 13, this shift register function is realized.

[0037] As may be seen in Fig. 5, the place values of the Galois elements a and b present at the bit place terminal a_{n-1} 23, bit place terminal a_{n-2} 24, bit place terminal b_{n-1} 25 and bit place terminal b_{n-2} 26, are multiplied out in the first to sixth XOR bit place multiplier elements 28, 30, 32, 34, 36, 38, and then assembled modulo additively place to place by the first to sixth XOR addition elements 27, 29, 31, 33, 35, 37 and made available at the first to fourth intermediate result terminals 39, 40, 41 and 42 for further processing at the reduction part 106. The term terminal herein is used to refer to a position in the circuit, and does not imply a connector, terminal pad or other structure.

[0038] The first and second and the fifth and sixth XOR adder elements 27, 29 and 35, 37 are each connected to an input with the first to fourth partial product adder expansion terminals 21, 22 and 43, 44. By way of these expansion terminals, these assembling XOR adder elements are connected with additional XOR adder elements of the partial product adder expansion structure 16, in which additional partial products of additional bit place values of the stored Galois elements a and b are assembled, which together with their product components enter into the place values of the intermediate result present at the first to fourth intermediate result terminals 39, 40, 41 ands 42.

[0039] As may be seen in Fig. 6, the apparatus realizes the algorithm of an MSB first Galois multiplier, and by way of the first to fourth reducer interim result terminals 49 to 52, the place values of a process intermediate result made available by the modulo reducer expansion structure 17 arrive in the modulo reducer key configuration 18, which performs the signal processing in two vertical processing planes.

[0040] In addition, by way of the connection of the first irreducible polynomial register terminal 45 and the second irreducible polynomial register terminal 46, the bit places PR_{n-1} and PR_{n-2} of the stored irreducible polynomial PR 9 are made available. These are therefore present at the first AND gate 53 and the third AND gate 57, and at the second AND gate 54 and fourth AND gate 58, and are gated with the respective processed MSB place values of the intermediate result Z.

[0041] These processed place values of the intermediate result Z at the same time form the MSB gate signals of the respective processing plane, and therefore the MSB gate signals for the AND connection of additional bit places of the irreducible polynomial PR 9. Hence the MSB gate signals firstly for the first processing plane are also present at an input of the second AND gate 54 and for further processing in the modulo reducer expansion structure 17 at the second reducer expansion terminal 62, and secondly for the second processing plane at an input of the fourth AND gate 58, and for further processing in the modulo reducer expansion structure 17 at the first reducer expansion terminal 61.

[0042] For the bit place PR_{n-1} of the stored irreducible polynomial PR 9, the MSB gate signal in the first processing plane represents the signal occupancy of the first reducer intermediate result terminal 49, and in the second processing plane, the modulo connection of the signal occupancy of the second reducer intermediate result terminal 50 made available by the first XOR connector 55 with the output signal of the first AND gate 53.

[0043] Further, the signal occupancy of the processed place values of the intermediate result Z, present at the third reducer intermediate result terminal 51, is modulo multiplied in the second XOR connector 56 with the output signal of the second AND gate 54, which makes available the AND connection of the MSB gate signal of the first processing plane with the bit place PR_{n-2} of the irreducible polynomial PR 9. Its output signal is applied to the inputs of the third XOR connector 59 for further modulo multiplication together with the output signal of the third AND gate 57, which performs the AND connection of the MSB gate signal of the second processing plane with the bit place PR_{n-1} of the irreducible polynomial PR 9. Its output signal in turn makes available the signal occupancy for the result terminal E_{n-1} 47.

[0044] Further, the signal occupancy of the processed place value of the intermediate result Z, present at the fourth reducer intermediate result terminal 52, is modulo multiplied in the fourth XOR connector 60 with the output signal of the fourth AND gate 58, which makes available the AND connection of the MSB gate signal of the second processing plane with the bit place PR_{n-2} of the irreducible polynomial PR 9. Its output signal makes available the signal occupancy for the result terminal E_{n-2} 48.

[0045] As may be seen in Fig. 7, the two-step adder key configuration 109 realizes the signal processing in two vertical planes in two horizontally divided adder steps. By way of the first to fourth intermediate result terminals 39 to 42, the place values of the intermediate result Z as made available by the two-step adder expansion structure 108 arrive in the two-step adder key configuration 109.

[0046] Besides, by way of the connection of the first irreducible polynomial register terminal 45 and second irreducible polynomial register terminal 46, the bit places PR_{n-1} and PR_{n-2} of the stored irreducible polynomial PR 9 as well as by way of the first preset register terminal 82 and the second preset register terminal 85, the bit places PE_{n-1} and PE_{n-2} of the stored expanded form PE 7 of the irreducible polynomial PR 9 arrive in the two-step adder key configuration 109.

[0047] The bit place Z_{n+1} of the intermediate result Z as made available by way of the first intermediate result terminal 39 is AND connected firstly at the input of the seventh cell gate 94 with the bit place PE_{n-1} of the expanded form PE 7 of the irreducible polynomial PR 9, and secondly at the input of the fifth cell gate 91 with the bit place PE_{n-2} of the expanded form PE 7 of the irreducible polynomial PR 9. The bit place Z_n of the intermediate result Z as made available by way of the second intermediate result terminal 40 is AND connected at the input of the eighth cell gate 95 likewise with the bit place PE_{n-2} of the expanded form PE 7 of the irreducible polynomial PR 9.

[0048] The outputs of the seventh and eighth cell gates 94, 95 are assembled in the first expansion gate 96, and then the sum signal present at its output is likewise modulo added in the second expansion adder 98 to an additional sum signal of the second processing plane of the two-step adder expansion structure 108, made available by way of the fifth reduction expansion terminal 81.

[0049] The output signal of the fifth cell gate 91 is modulo added to an additional sum signal of the first processing plane of the two-step adder expansion structure 108, made available by way of the sixth reduction expansion terminal 84, at the input of the third expansion adder 92. The output signal of the third expansion adder 92 forms the MSB gate signal of the first processing plane, and is then firstly connected to the sixth cell gate 93 and secondly applied to the ninth reduction expansion terminal 86, to afford an additional processing in the first processing plane of the two-step adder expansion structure 108.

[0050] The output of the second expansion adder 98 forms the MSB gate signal of the second processing plane, and for that purpose is connected firstly to the inputs of the ninth cell gate 97 and the tenth cell gate 101, and secondly to the tenth reduction expansion terminal 89, to afford further processing in the second processing plane of the two-step adder expansion structure 108.

[0051] The output signal of the third expansion adder 93 is AND connected in the sixth cell gate 93 with the bit place PR_{n-2} of the stored irreducible polynomial PR 9, present by way of the second irreducible polynomial register terminal 46. The output signal of the second expansion adder 98 is AND connected in the ninth cell gate 97 to the bit place PR_{n-1} of the stored irreducible polynomial PR 9, present by way of the first irreducible polynomial register terminal 45. With its output signal and the output signal of the sixth cell gate 93, a modulo addition takes place in the second output adder 100.

[0052] A modulo addition takes place likewise with the signal occupancy of the third intermediate result terminal 41 and the signal occupancy of the seventh reduction expansion terminal 87 in the first output adder 99. Its output signal is modulo added to the output signal of the second output adder 100 in the third output adder 102, and, with its output signal, forms the signal occupancy of the result register terminal E_{n-1} 47.

[0053] The output signal of the second expansion adder 98 is AND connected in the tenth cell gate 101 to the bit place PR_{n-2} of the stored irreducible polynomial PR 9, present by way of the second irreducible polynomial register terminal 46. Its output signal is modulo added to the signal occupancy of the fourth intermediate result terminal 42 in the fourth output adder 103. This output signal is modulo added to the signal occupancy of the eighth reduction expansion terminal 88 in the fifth output adder 104, and, with its output signal, forms the signal occupancy of the result register terminal E_{n-2} 48.

[0054] As may be seen in Fig. 8, the one-step adder key configuration 112 realizes the signal processing in two vertical planes and in only one horizontally unfolded adder step. By way of the first to fourth intermediate result terminals 39 to 42, the place values of the intermediate result Z as made available by the one-step adder expansion structure 111 arrives in the one-step adder key configuration 112.

[0055] Besides, by way of the first PEM terminal 65, second PEM terminal 66, third PEM terminal 63 and fourth PEM terminal 78, the bit places $PE_{n-2,0}$ and $PE_{n-1,0}$ as well as $PE_{n-2,1}$ and $PE_{n-1,1}$ of the stored matrix PEM 11 of the expanded form PE 7 of the irreducible polynomial PR 9 arrive in the one-step adder key configuration 112.

[0056] The bit place Z_{n+1} of the intermediate result Z as made available by way of the first intermediate result terminal 39 is AND connected firstly at the input of the second cell gate 68 to the bit place $PE_{n-2,0}$ of the matrix PEM 11, and secondly at the input of the first cell gate 67 to the bit place $PE_{n-2,1}$ of the matrix PEM 11.

[0057] The bit place Z_n of the intermediate result Z as made available by way of the second intermediate result terminal 40 is AND connected firstly at the input of the fourth cell gate 70 to the bit place $PE_{n-1,0}$ of the matrix PEM and secondly at the input of the third cell gate 69 to the bit place $PE_{n-1,1}$ of the matrix PEM 11.

[0058] A modulo addition takes place with the signal occupancy of the third intermediate result terminal 47 and the output signal of the fourth cell gate 70 in the second XOR partial adder 72.

[0059] With the signal occupancy of the third reduction expansion terminal 64 and the output signal of the second cell gate 68, a modulo addition takes place in the first XOR partial adder 71. Its output signal is likewise modulo added in the third XOR partial adder 73 to the output signal of the second XOR partial adder 72, and, with its output signal, forms the signal occupancy of the result register terminal E_{n-1} 47. A further modulo addition takes place with the signal occupancy of the fourth intermediate result terminal 42 and the output signal of the third cell gate 69 in the fifth XOR partial adder 75. With the signal occupancy of the fourth reduction expansion terminal 77 and the output signal of the first cell gate 67, a modulo addition takes place in the fourth XOR partial adder 74. Its output signal is modulo added likewise to the output signal of the fifth XOR partial adder 75 in the sixth XOR partial adder 76, and, with its output signal, forms the signal occupancy of the result register terminal E_{n-2} 48.